IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	10/699,005
Filing Date:	10/30/2003
Applicant(s):	Michael Scheidell
Entitled:	INTRUSION DETECTION SYSTEM
Examiner:	Sherkat, Arezoo
Group Art Unit:	2431
Attorney Docket No.:	1012-003U

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is Appellant's Appeal Brief in support of the Notice of Appeal filed May 13, 2009. This Appeal Brief has been timely filed within the statutory period from the filing of the Notice of Appeal. No fee is due with this Appeal Brief because Appellants have previously paid the Appeal Brief fee on 08-21-2008. Notwithstanding, please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-3829, and please credit any excess fees to such deposit account.

Date: June 4, 2009

Respectfully submitted,

/Steven M. Greenberg/
Steven M. Greenberg, Registration No. 44,725
Mark. P. Terry, Registration No. 47,133
Customer Number 29973
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, FL 33487
Tel: (561) 922-3845

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	10/699,005
Filing Date:	10/30/2003
Applicant(s):	Michael Scheidell
Entitled:	INTRUSION DETECTION SYSTEM
Examiner:	Sherkat, Arezoo
Group Art Unit:	2431
Attorney Docket No.:	1012-003U

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed May 13, 2009, wherein Appellants appeal from the Examiner's rejection of claims 9 through 11 and 14 on Nov. 12, 2008 (the "Office Action").

I. REAL PARTY IN INTEREST

This application is assigned to SecNAP Network Security, LLC by assignment recorded on October 31, 2002, at Reel 013451, Frame 0050.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals and interferences.

III. STATUS OF CLAIMS

Claims 1 through 8, 12, 13 and 15 through 20 have been canceled. Claims 9 through 11 and 14 remain pending in this Application and have been four times rejected. It is from the multiple rejections of claims 9 through 11 and 14 that this Appeal is taken.

IV. STATUS OF AMENDMENTS

Claims 9 through 11 have not been amended since the imposition of the Office Action dated November 12, 2008. Claim 14 has been amended by way of an Amendment submitted by Appellant on May 12, 2009, subsequent to the imposition of the Office Action dated November 12, 2008.

V. SUMMARY OF CLAIMED SUBJECT MATTER

As set forth in the Abstract of Appellant's published specification, claims 9 and 14 are directed to an intrusion detection system (IDS). In Appellant's invention, the IDS monitors the rate and characteristics of Internet attacks on a computer network and filters attack alerts based upon various rates and frequencies of the attacks. The IDS also monitors attacks on other hosts and determines if the attacks are random or general attacks or attacks directed towards a specific computer network and generates a corresponding signal. Finally, the IDS tests a computer network's vulnerability to attacks detected on the other monitored hosts.

With specific reference to claim 9, a computer network intrusion detection system can include different log analyzers for different external networks. (Par. [0042]) Each log analyzer can be configured for detecting attacks upon a firewall in a corresponding one of the different

external networks defining an edge detection network. (Par. [0042]) An edge database log can be coupled to the different log analyzers logging attacks upon the different external networks. (Par. [0042]) Further, an intrusion detector can be coupled to a client network and configured to detect external attacks upon the client network. (Par. [0042]) An analyzer also can be coupled to the intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log. (Par. [0045]) Finally, a filter can be coupled to the analyzer for generating an alert based upon characteristics of a plurality of attacks. (Par. [0046])

The system also can include a second intrusion detector for detecting external attacks upon a second computer network. (Par. [0045]) Correspondingly, a second analyzer can be coupled to the second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof. (Par. [0045]) As such, the filter can be further coupled to the second analyzer. (Par. [0045]) When coupled to the second analyzer, the filter further compares the attack characteristics determined by the analyzer and the second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison. (Par. [0045])

With respect to claim 14, a method of generating a network intrusion alert for a first network coupled to a multiple client network system can be provided. (Par. [0047]) The method can include logging attacks on multiple different external networks defining an edge detection network (Par. [0055]), detecting an attack on a client network (Par. [0055]), classifying the attack

as either a general attack or a client specific attack (Par. [0055]) by comparing the attack to attacks logged for the edge detection network (Par. [0055]), and prioritizing handling of the detected attack if the attack is classified as a general attack. (Par. [0055]). The method further includes generating a first alert in response to an absence of a match between the attack and the attacks logged for the edge detection network, wherein the first alert is indicative of a client specific attack on the first network. (Par. [0055]) Lastly, the method includes generating a second alert in response to the presence of a match between the attack and the attacks logged for the edge detection network, wherein the second alert is indicative of a general attack on the first network. (Par. [0055]).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 9 through 11 and 14 are not anticipated by U.S. Patent No. 6,971,028 to Lyle (hereinafter "Lyle") under 35 U.S.C. § 102(e).

VII. THE ARGUMENT

THE REJECTION OF CLAIMS 9 THROUGH 11 AND 14 UNDER 35 U.S.C. § 102(E)

The factual determination of anticipation under 35 U.S.C. § 102 requires the identical disclosure, either explicitly or inherently, of each element of a claimed invention in a single reference.[1] Moreover, the anticipating prior art reference must describe the recited invention with sufficient clarity and detail to establish that the claimed limitations existed in the prior art and

[1] In re Schreiber, 128 F.3d 1473, 1477 (Fed. Cir. 1997) ("To anticipate a claim, a prior art reference must disclose every limitation of the claimed invention, either explicitly or inherently"), In re Rijckaert, 9 F.3d 1531, 28 USPQ2d 1955 (Fed. Cir. 1993); Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989); Perkin-Elmer Corp. v. Computervision Corp., 732 F.2d 888, 894, 221 USPQ 669, 673 (Fed. Cir. 1984).

that such existence would be recognized by one having ordinary skill in the art.[2] Absence from an allegedly anticipating prior art reference of any claimed element negates anticipation.[3]

"Both anticipation under § 102 and obviousness under § 103 are two-step inquiries. The first step in both analyses is a proper construction of the claims. ... The second step in the analyses requires a comparison of the properly construed claim to the prior art."[4] During patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification,"[5] and the broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach.[6] Therefore, the Examiner must (i) identify the individual elements of the claims and properly construe these individual elements,[7] and (ii) identify corresponding elements disclosed in the allegedly anticipating reference and compare these allegedly corresponding elements to the individual elements of the claims.[8] This burden has not been met.

1. Examiner Failed to Properly Construe Claim Limitations Integral to the Claims

A critical aspect of Examiner's function as the trier of fact in examining the claims of a patent application is to first perform a claim construction of the terms of the claims. Examiner has failed to expressly do so in the Office Action dated Nov. 12, 2008.

---

[2] See In re Spada, 911 F.2d 705, 708, 15 USPQ 1655, 1657 (Fed. Cir. 1990); Diversitech Corp. v. Century Steps Inc., 850 F.2d 675, 678, 7 USPQ2d 1315, 1317 (Fed. Cir. 1988).

[3] Kloster Speedsteel AB v. Crucible, Inc., 793 F.2d 1565, 1571 (Fed. Cir. 1986)(emphasis added).

[4] Medichem, S.A. v. Rolabo, S.L., 353 F.3d 928, 933 (Fed. Cir. 2003) (internal citations omitted).

[5] In re ICON Health and Fitness, Inc., 496 F.3d 1374, 1379 (Fed. Cir. 2007) ("[T]he PTO must give claims their broadest reasonable construction consistent with the specification. Therefore, we look to the specification to see if it provides a definition for claim terms, but otherwise apply a broad interpretation."); In re Hyatt, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000).

[6] In re Cortright, 165 F.3d 1353, 1359, 49 USPQ2d 1464, 1468 (Fed. Cir. 1999)

[7] See also, Panduit Corp. v. Dennison Mfg. Co., 810 F.2d 1561, 1567-68 (Fed. Cir. 1987) (In making a patentability determination, analysis must begin with the question, "what is the invention claimed?" since "[c]laim interpretation,. . . will normally control the remainder of the decisional process"); see Gechter v. Davidson, 116 F.3d 1454, 1460 (Fed. Cir. 1997) (requiring explicit claim construction as to any terms in dispute).

[8] Lindermann Maschinenfabrik GMBH v. American Hoist & Derrick Co., 730 F.2d 1452, 221 USPQ 481 (Fed. Cir. 1984).

A. Claim Construction of "General Attack" and "Client Specific Attack"

In construing the claim terms "general attack" and "client specific attack" of independent claims 9 and 14, the Examiner compares the aforementioned claim terms to the terms "group of related events" and "events not related to any other events" of Lyle. Specifically, on p. 3 of the Office Action, the Examiner asserts that the claim terms "general attack" and "client specific attack" are found in col. 7 line 43 to col. 8 line 14 of Lyle, which is reproduced in its entirety for the convenience of the Honorable Board below:

> When information related to an actual or suspected attack is received by the handoff receiver 302 or identified by the sniffer module 304, the relevant information is provided to an event manager module 306. The event manager 306 receives the suspicious data, referred to herein as "event" data, places it in a queue, and provides data to the analysis framework module 308 for processing, one event at a time, at predetermined intervals. The event manager 306 also supplies event data to the log database 320 as it is received either from the handoff receiver 302 or from the sniffer module 304. The event data stored in log database 320 may then be used for post-attack analysis or it may be shared with other tracking systems installed in the same administrative domain in which the tracking system in which the event manager 306 is located, or with tracking systems in other administrative domains, as described more fully below.
>
> The analysis framework 308 processes event data, determines the appropriate course of responsive action, and takes the responsive action, if any. The analysis framework 308 associates the event data with an event software object, as described more fully below, and stores data relating to the event in an event database 322. The analysis framework 308 also determines whether an event is associated with an existing event or group of related events, and associates related events into a single incident software object. Events that are not related to any other events are associated with a new incident object and may be later grouped with subsequently-received event data that is related to the same incident.
>
> One of the tools used by analysis framework 308 in determining whether an event is associated with one or more other events is a statistics database 324. The statistics database 324 stores the average incident rate of each sub-network within the network served by the tracking system and a first-order variance of the average incident rate for all networks with an above-average incident rate. The baseline incident rate and the variance are used for all networks with an average or below-average incident rate. (emphasis added)

A reading of the passage cited by the Examiner above reveals that the Examiner has implicitly construed Appellant's claimed limitations "general attack" and "client specific attack" to mean "group of related events" and "events not related to any other events," as defined by Lyle in the passage above. The plain meaning of "general attack," however, is an attack that is

general in nature, while the plain meaning of "client specific attack" is an attack that is client-specific in nature. The plain meaning of the aforementioned claim terms does not coincide with the meaning ascribed to them by the Examiner. A proper construction of the aforementioned claims terms should be the plain meaning of the claim terms, as defined above, resulting in a reasonable interpretation of the claim terms. The broadest reasonable interpretation of "general attack" and "client specific attack" set forth above is fully consistent with Appellant's use of the terms in Appellant's specification as evidenced by paragraph [0032] of Appellant's specification as follows:

> [0032] Given the large number of attacks that may be experienced by a client, it is desirable to determine if the attack is a general attack or a specific attack directed at the particular client.

The Examiner has therefore erred in construing the claim terms "general attack" and "client-specific attack."

B. Claim Construction of "Specific Attack Alert"

With regard to the claim term "specific attack alert" of independent claim 9 and the claim term "alert … indicative of a client specific attack" of independent 14, the Examiner provides no claim construction of these claim terms and the Examiner does not assert that Lyle discloses these claim terms. Specifically, on p. 4 of the Office Action, the Examiner asserts that Appellant's claim elements "wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison" are found in col. 7 line 43 to col. 8 line 33 of Lyle. Note that col. 7 line 43 to col. 8 line 14 of Lyle is reproduced above. Thus, col. 8 lines 14-33 of Lyle is reproduced in its entirety for the convenience of the Honorable Board below:

> The analysis framework 308 also connects to a policy database 326. The policy database 326 is used to store information concerning how certain types of events and incidents should be processed by the analysis framework, including the responsive action, if any, to be taken by the analysis framework. For example, for a particular type of attack or suspected attack the policy database 326 may indicate that the attack is to be logged but otherwise ignored. For a different type of attack, the policy database 326 may indicate that an alert should be sent to a designated individual or group of individuals. In such a case, the analysis framework 308 sends a request to an alerting module 310. Alerting module 310 then sends the required alert by the appropriate means. In one embodiment, the alerting module 310 sends an e-mail message to a network security administrator advising the network security administrator of the alert condition. In one embodiment, the alerting module 310 is configured to send an alert to the network security administrator via a pager. (emphasis added)

Because the Examiner provides no claim construction of the claim terms "specific attack alert" and "alert … indicative of a client specific attack" as required by under 35 U.S.C. § 102, the Examiner's rejection of claims 9-1 and 14 is not viable. For the purposes of fully responding to the Examiner's rejection, however, the Appellant will generously assume that the Examiner meant to construe Appellant's claim terms "specific attack alert" and "alert … indicative of a client specific attack" to mean "an alert … sent to a designated individual or group of individuals," as defined in the passage of Lyle above.

The plain meaning of "specific attack alert" and "alert … indicative of a client specific attack," however, is an alert that indicates an attack that is client-specific in nature. The plain meaning of the aforementioned claim terms does not coincide with the meaning presumptively ascribed to them by the Examiner. A proper construction of the aforementioned claims terms should be the plain meaning of the claim terms, as defined above, resulting in a reasonable interpretation of the claim terms. The broadest reasonable interpretation of "specific attack alert" and "alert … indicative of a client specific attack" set forth above is fully consistent with Appellant's use of the terms in Appellant's specification as evidenced by paragraph [0055] of Appellant's specification as follows:

> [0055] … Client specific attacks preferably receive more urgent treatment because of the more invidious nature of the attack. By comparing the characteristic of attacks upon a client network

with those of the edge network, it can be determined if the attack is general or specific and the priority of the alert adjusted accordingly. The invention's ability to quickly and automatically identify and alert a specific attack has significant advantages in intrusion detection and corresponding responses in protecting the client network.

The Examiner has therefore erred in construing the claim terms "specific attack alert" and "alert … indicative of a client specific attack."

2. Examiner Failed to Properly Compare Teachings of Lyle with Limitations of Claims

For the convenience of the Honorable Board, claims 10 and 11 stand or fall together with claim 9 and independent claim 14 stands or falls alone. With respect to claim 9, a computer network intrusion detection system has been recited. A complete reproduction of claim 9 is reproduced herein in its entirety:

9. A computer network intrusion detection system comprising:
a plurality of different log analyzers for different external networks, each log analyzer being configured for detecting attacks upon a firewall in an corresponding one of the different external networks defining an edge detection network;
an edge database log coupled to the different log analyzers logging attacks upon the different external networks;
an intrusion detector coupled to a client network and configured to detect external attacks upon the client network;
an analyzer coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log; and,
a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks;
a second intrusion detector for detecting external attacks upon a second computer network; and,
a second analyzer coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof, wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison.

14. A method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:
logging attacks on multiple different external networks defining an edge detection network;
detecting an attack on a client network;
classifying the attack as either a general attack or a client specific attack by comparing the attack to attacks logged for the edge detection network;
prioritizing handling of the detected attack if the attack is classified as a general attack;
generating a first alert in response to an absence of a match between the attack and the

attacks logged for the edge detection network, wherein the first alert is indicative of a client specific attack on the first network; and

generating a second alert in response to a presence of a match between the attack and the attacks logged for the edge detection network, wherein the second alert is indicative of a general attack on the first network.

Integral to the system and method of independent claims 9 and 14 is the step of classifying an attack as either a general attack or a specific attack. Further integral to the system and method of independent claims 9 and 14 is the step of comparing attack characteristics, such as to find a match. Further integral to the system and method of independent claims 9 and 14 is the step of providing an alert indicative of a client specific attack. These limitations cannot be found in Lyle.

A. Comparison of Claim Limitation "Classifying the attack as either a general attack or a client specific attack"

Given Examiner's misconstruction of the essential claim terms "general attack" and "client specific attack" present in independent claims 9 and 14, Examiner has failed to locate the identical disclosure, either explicitly or inherently, of each element of Appellant's claimed invention in a single reference as required by law. For this reason, the Examiner's rejection of claims 9-11 and 14 under 35 U.S.C. § 102 should be reversed. Even if Examiner had properly construed the aforementioned claim terms, however, Lyle does not provide an identical disclosure of the claim element "classifying the attack as either a general attack or a client specific attack."

On p. 3 of the Office Action, the Examiner asserts that the claim element above is found in col. 7 line 43 to col. 8 line 14 of Lyle, which is reproduced above in its entirety for the convenience of the Honorable Board. A reading of the passage cited by the Examiner, however,

reveals that Lyle does not disclose the step of classifying an attack as "general" or "client specific." At best, Lyle discloses the determination of whether event data is or is not related to other event data stored in a database. Classifying event data as related to not related to other event data stored in a database, IS THE NOT SAME AS "classifying the attack as either a general attack or a client specific attack." Lyle does not disclose that any determination is made regarding classifying the event data as a "general attack" or a "client specific attack," as claimed by Appellant.

The Examiner has therefore erred in comparing the claim element "classifying the attack as either a general attack or a client specific attack" with the determination of whether event data is or is not related to other event data stored in a database, as disclosed by Lyle. Thus, the Examiner has failed to locate the identical disclosure, either explicitly or inherently, of each element of Appellant's claimed invention in a single reference as required by law. Accordingly, Examiner has failed to present a prima facie case of anticipation in respect to claims 9 through 11 and 14. For this additional reason, the Examiner's rejection of claims 9-11 and 14 under 35 U.S.C. § 102 should be reversed.

B. Comparison of Claim Limitation "Compares the attack characteristics ..."

Lyle does not provide an identical disclosure of the claim term "compares the attack characteristics determined by said analyzer and said second analyzer" of independent claim 9 and the claim term "match between the attack and the attacks logged for the edge detection network" of independent claim 14, wherein both claim terms refer to the comparison of characteristics of a first attack with characteristics of a second attack.

On p. 4 of the Office Action, the Examiner asserts that the claim elements above are found in col. 7 line 43 to col. 8 line 33 of Lyle, which is reproduced above in its entirety for the convenience of the Honorable Board. A reading of the passage cited by the Examiner, however, reveals that Lyle does not disclose the comparison of characteristics of a first attack with characteristics of a second attack. At best, Lyle discloses the determination of whether event data is or is not related to other event data stored in a database. Classifying event data as related to not related to other event data stored in a database, IS THE NOT SAME AS comparing characteristics of a first attack with characteristics of a second attack. Lyle does not disclose that any comparison is made between characteristics of attacks, as claimed by Appellant.

The Examiner has therefore erred in comparing the claim terms "compares the attack characteristics determined by said analyzer and said second analyzer" of independent claim 9 and the claim term "match between the attack and the attacks logged for the edge detection network" of independent claim 14 with the determination of whether event data is or is not related to other event data stored in a database, as disclosed by Lyle. Thus, the Examiner has failed to locate the identical disclosure, either explicitly or inherently, of each element of Appellant's claimed invention in a single reference as required by law. Accordingly, Examiner has failed to present a prima facie case of anticipation in respect to claims 9 through 11 and 14. For this additional reason, the Examiner's rejection of claims 9-11 and 14 under 35 U.S.C. § 102 should be reversed.

C. Comparison of Claim Limitation "Generates a specific attack alert ..."

Given Examiner's misconstruction of the essential claim term "specific attack alert" present in independent claim 9, Examiner has failed to locate the identical disclosure, either

explicitly or inherently, of each element of Appellant's claimed invention in a single reference as required by law. For this additional reason, the Examiner's rejection of claim 9 under 35 U.S.C. § 102 should be reversed. Even if Examiner had properly construed the aforementioned claim term, however, Lyle does not provide an identical disclosure of the claim term "generates a specific attack alert in response to a substantial absence of similarity in the comparison" of independent claim 9 and the claim term "generating a first alert in response to an absence of a match between the attack and the attacks logged for the edge detection network, wherein the first alert is indicative of a client specific attack" of independent claim 14, wherein both claim terms refer to generating a client specific attack alert if the current attack does not match previous attacks.

On p. 4 of the Office Action, the Examiner states the following about the claim elements above:

> "generating a specific attack alert ..." is merely a policy that, as a design choice, may well be defined in the policy database 326. The policy database is therefore consulted to dictate how certain types of events and incidents should be processed by the analysis framework 308, including the responsive action, if any, to be taken by the analysis framework. Therefore, depending on the defined policy the alerting module is instructed to generate alerts based on different triggering events."

Other than the ambiguous statement above, the Examiner makes no other statement about the claim elements above. The Examiner does not cite a column number or line number in Lyle and the Examiner does not recite a passage or a figure of Lyle. In fact, the Examiner does not even assert that Lyle explicitly discloses the aforementioned claim elements, as required by law. At best, the Examiner states that the aforementioned claim elements "may well be defined in the policy database." As explained above, under 35 U.S.C. § 102 requires the identical disclosure, either explicitly or inherently, of each element of a claimed invention in a single reference. Moreover, the anticipating prior art reference must describe the recited invention with sufficient

clarity and detail to establish that the claimed limitations existed in the prior art and that such existence would be recognized by one having ordinary skill in the art. Because the Examiner has not met this burden, the Examiner's rejection of claims 9-11 and 14 under 35 U.S.C. § 102 is not viable and should be reversed.

In order to fully respond to the Examiner's rejection, however, the Appellant will generously assume that the Examiner meant to assert that the aforementioned claim elements are found in col. 8 lines 15-53 of Lyle, which is reproduced below in its entirety for the convenience of the Honorable Board.

> The analysis framework 308 also connects to a policy database 326. The policy database 326 is used to store information concerning how certain types of events and incidents should be processed by the analysis framework, including the responsive action, if any, to be taken by the analysis framework. For example, for a particular type of attack or suspected attack the policy database 326 may indicate that the attack is to be logged but otherwise ignored. For a different type of attack, the policy database 326 may indicate that an alert should be sent to a designated individual or group of individuals. In such a case, the analysis framework 308 sends a request to an alerting module 310. Alerting module 310 then sends the required alert by the appropriate means. In one embodiment, the alerting module 310 sends an e-mail message to a network security administrator advising the network security administrator of the alert condition. In one embodiment, the alerting module 310 is configured to send an alert to the network security administrator via a pager.
>
> For certain types of events and incidents, the policy database 326 may indicate that the analysis framework 308 should track the attack back to determine the point of attack at which the messages from the attacking party are entering the network or sub-network associated with the tracking system. In such cases, the analysis framework 308 consults a topology database 328. The topology database 328 contains information concerning the devices which comprise the network or sub-network associated with the tracking system and how those devices are configured and connected to one another to form the network or sub-network associated with the tracking system. The analysis framework 308 uses this information to create a virtual map of the network. The analysis framework then uses this map to systematically track to the source of the attack to identify the point of the attack. In one embodiment, to track back the source of an attack the analysis framework 308 instructs one or more of the sniffers that comprise sniffer module 304 to systematically search ports on network devices until the point of attack has been identified, as described more fully below.

A reading of the passage above, however, reveals that Lyle does not disclose generating a client specific attack alert if the current attack does not match previous attacks. At best, Lyle discloses specifying how a system responds to certain events, including sending alerts. Specifying how a

system responds to certain events, including sending alerts, however, IS THE NOT SAME AS generating a client specific attack alert if the current attack does not match previous attacks. Lyle does not disclose that any comparison is made between characteristics of attacks so as to determine whether a client specific attack alert is sent, as claimed by Appellant.

The Examiner has therefore erred in comparing the claim term "generates a specific attack alert in response to a substantial absence of similarity in the comparison" of independent claim 9 and the claim term "generating a first alert in response to an absence of a match between the attack and the attacks logged for the edge detection network, wherein the first alert is indicative of a client specific attack" of independent claim 14, with specifying how a system responds to certain events, including sending alerts, as disclosed by Lyle. Thus, the Examiner has failed to locate the identical disclosure, either explicitly or inherently, of each element of Appellant's claimed invention in a single reference as required by law. Accordingly, Examiner has failed to present a prima facie case of anticipation in respect to claims 9 through 11 and 14. For this additional reason, the Examiner's rejection of claims 9-11 and 14 under 35 U.S.C. § 102 should be reversed.

In view of the foregoing, Appellant respectfully submits that the Examiner's rejections under 35 U.S.C. § 102(e) based upon the applied prior art are not viable as Examiner has completely misconstrued several important claim terms present in Appellant's claims, and Examiner has failed to compare the properly construed claims to the prior art. Appellants, therefore, respectfully solicit the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. § 102(e).

Date: June 4, 2009

Respectfully submitted,

/Steven M. Greenberg/
Steven M. Greenberg
Registration No. 44,725
Mark P. Terry
Registration No. 47,133
Customer Number 29973
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, FL 33487
Tel: (561) 922-3845
Facsimile: (561) 244-1062

VIII. CLAIMS APPENDIX

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Previously Amended) A computer network intrusion detection system comprising:

a plurality of different log analyzers for different external networks, each log analyzer being configured for detecting attacks upon a firewall in an corresponding one of the different external networks defining an edge detection network;

an edge database log coupled to the different log analyzers logging attacks upon the different external networks;

an intrusion detector coupled to a client network and configured to detect external attacks upon the client network;

an analyzer coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log; and,

a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks;

a second intrusion detector for detecting external attacks upon a second computer network; and,

a second analyzer coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof, wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison.

10. (Original) The system according to claim 9 further comprising an alert generator for generating an alert indicative of the specific attack on the one of the networks experiencing the attacks having the absence of similarity of attacks on the other of the networks.

11. (Original) The system according to claim 9 further comprising: a vulnerability tester coupled to said filter for testing the one of the networks not experiencing the attacks for a vulnerability to the attack characteristic experienced by the other of the computer networks.

12. (Cancelled)

13. (Cancelled)

14. (Previously Amended) A method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:

logging attacks on multiple different external networks defining an edge detection network;

detecting an attack on a client network;

classifying the attack as either a general attack or a client specific attack by comparing the attack to attacks logged for the edge detection network;

prioritizing handling of the detected attack if the attack is classified as a general attack;

generating a first alert in response to an absence of a match between the attack and the attacks logged for the edge detection network, wherein the first alert is indicative of a client specific attack on the first network; and

generating a second alert in response to a presence of a match between the attack and the attacks logged for the edge detection network, wherein the second alert is indicative of a general attack on the first network.

15. (Cancelled)

16. (Cancelled)

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

IX. EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

X. RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.